Deutscher Bundestag **Drucksache 18/10870**

18. Wahlperiode 18.01.2017

Vorabfassung - wird durch die lektorierte Version ersetzt.

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/10717 –

Weiteres Datenleck bei der EU-Polizeiagentur Europol

Vorbemerkung der Fragesteller

Nach Berichten des niederländischen Fernsehsenders ZEMBLA gelangten vertrauliche Informationen der EU-Polizeiagentur Europol in Den Haag ins Internet. Eine Mitarbeiterin hat demnach eingestufte Informationen mit nach Hause genommen und digitale Kopien auf einem Netzlaufwerk angefertigt. Der Datenträger von Lenovo sei mit dem Internet verbunden gewesen. Laut Wil van Gemert, dem ehemaligen niederländischen Geheimdienstchef und jetzigen stellvertretenden Direktor von Europol, ist nicht ausgeschlossen, dass außer dem Sender weitere Parteien Einblick in die Daten gehabt hätten. Eine Untersuchung soll nun klären, warum die von der niederländischen Polizei zu Europol entsandte Mitarbeiterin die Daten mitnahm und kopierte. Die Frau arbeitete bereits seit elf Jahren für Europol. Laut einem Sprecher von Europol verfüge die Agentur eigentlich über ein „sehr robustes System“, um die gespeicherten Informationen zu schützen. Deshalb sollten nun die Sicherheitsprotokolle überprüft werden.

Bereits im Jahr 2012 kamen Europol Daten abhanden; auch damals wurden diese auf einem Netzlaufwerk gespeichert (www.computable.nl vom 10. Dezember 2012, „Orange blundert bij Europol met Iomega-lek“). Laut dem britischen Sender BBC vom 30. November 2016 nimmt der noch amtierende Europol-Direktor Rob Wainwright, ein ehemaliger Analyst des Geheimdienstes MI5, jetzt an einem Seminar zu Onlinesicherheit und Datenschutz teil („Secret Europol terror data found online“).

1. Wie bewertet die Bundesregierung die derzeitige Sicherheit der auch von deutschen Behörden gelieferten sensiblen Informationen bei Europol?

Die Bundesregierung bewertet die Sicherheit der an Europol gelieferten bzw. dort verwahrten sensiblen Informationen grundsätzlich positiv.

Der Ratsbeschluss 2009/371/JI zur Errichtung des Europäischen Polizeiamtes (Europol) regelt in drei Artikeln (40, 41 und 46) die Notwendigkeit des Schutzes

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 17. Januar 2017 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

sensibler und eingestufter Informationen, die jeweiligen Verantwortlichkeiten aller bei oder durch Europol Beschäftigten sowie die Anbindung dieser Schutzmaßnahmen an das jeweilige nationale Recht der Europol-Mitgliedstaaten.

Artikel 40 bestimmt insbesondere, dass der Rat spezielle, Europol betreffende Sicherheitsregeln zu verabschieden hat und Personen, die bei Europol Umgang mit eingestuften Informationen haben, sich zuvor erfolgreich einer Sicherheitsüberprüfung auf Basis des jeweiligen nationalen Sicherheitsüberprüfungsrechts unterziehen müssen.

Artikel 41 bestimmt unter anderem die Pflicht zur Amtsverschwiegenheit und weist im Falle von Verstößen dagegen den Mitgliedstaaten die Pflicht zu, diese Verstöße als Verstöße gegen das jeweilige nationale Recht über die Amtsverschwiegenheit bzw. über den Schutz eingestufter Informationen zu behandeln.

Artikel 46 bestimmt schließlich, dass sich der Schutz von EU-Verschlusssachen (EUCI) bei Europol an den Grundsätzen und Mindestanforderungen orientiert, die der Beschluss des Rates zur Annahme seiner eigenen Sicherheitsvorschriften (2013/488/EU) festlegt.

Die nach Maßgabe des Artikels 40 erlassenen Europol-Sicherheitsregeln (2009/968/JI) entsprechen den derzeit gültigen Standards und werden, soweit notwendig, angepasst. So schreiben diese Regeln neben den klassischen vier Einstufungsgraden auch das so genannte „Basic Protection Level“ (Artikel 10) vor. Dabei handelt es sich um einen Schutzgrad, der auf alle durch Europol gehandhabten Informationen anzuwenden ist, die nicht explizit als für die Öffentlichkeit bestimmt gekennzeichnet sind. Genaue Handlungsanweisungen dazu werden im sogenannten Europol Sicherheitshandbuch festgelegt.

Die von Europol betriebenen IT-Systeme durchlaufen in regelmäßigen Abständen eine Sicherheitsbewertung (Security Assessment) und Akkreditierung.

2. Wann und von wem wurde die Bundesregierung über das jüngste Datenleck bei der EU-Polizeiagentur Europol informiert, und welchen Inhalt hatte diese erste Mitteilung?

Das deutsche Verbindungsbüro bei Europol wurde am 26. Oktober 2016 durch Europol über den Sicherheitsvorfall und den Stand der Ermittlungen von Europol unterrichtet.

3. Welche weiteren Mitteilungen erfolgten seitdem, und welchen Inhalt hatten diese?

Am 27. Oktober 2016 wurden dem deutschen Verbindungsbüro die betroffenen Daten zur Prüfung und Bewertung zugeleitet. Am 31. Oktober 2016 wurden die Mitgliedstaaten im Europol-Sicherheitsausschuss informiert. Der Europol-Verwaltungsrat wurde mit Schreiben des Vorsitzenden vom 30. November 2016 über den Hintergrund des Sicherheitsvorfalls und den aktuellen Verfahrensstand unterrichtet. Ferner nahm Europol eine allgemeine Bewertung vor. Auf dieser Grundlage war der Vorfall auch Gegenstand des Europol-Verwaltungsrates am 13. Dezember 2016.

Vorabfassung - wird durch die lektorierte Version ersetzt.

4. Auf welchem Weg bzw. über welche Datenträger gelangten die Daten nach Kenntnis der Bundesregierung ins Internet und schließlich zum Fernsehsender Zembla, und wer ist nach gegenwärtigem Stand der Erkenntnisse für das Datenleck verantwortlich?

Die Bundesregierung kann vor Abschluss der derzeit laufenden Untersuchung des Vorfalls dazu keine Angaben machen.

5. Inwiefern trifft nach Kenntnis der Bundesregierung der TV-Medienbericht von Zembla vom 30. November 2016 zu oder nicht zu, wonach die Polizeibeamtin die Daten zuerst auf einen USB-Stick kopierte, diese anschließend auf ihrem Laptop speicherte und die Daten des Laptop schließlich als Sicherungskopie auf das Netzlaufwerk gelangten?

Auf die Antwort zu Frage 4 wird verwiesen.

6. Für welche Datenbestände (etwa das Europol-Informationssystem oder die Analysedateien) bei Europol ist es nach Kenntnis der Bundesregierung technisch möglich, diese auf ein externes Laufwerk zu kopieren, und für welche Datenbestände ist dies nicht möglich?

Der Bundesregierung ist nicht bekannt, für welche Datenbestände und welchen Personenkreis bei Europol es derzeit technisch möglich ist, Daten auf ein externes Laufwerk zu kopieren.

7. Wie viele Datensätze in welcher Größe und zu wie vielen Ermittlungen waren nach Kenntnis der Bundesregierung von dem jüngsten Datenleck betroffen?

   a) Aus welchen Europol-Dateien stammten die abhandengekommenen Daten?

   b) Welche Einstufungen trugen diese?

   c) Welche Tatkomplexe waren vornehmlich betroffen?

   d) Wie viele Personendatensätze enthielten die Daten?

   e) Wie viele der abhandengekommenen Daten stammten von deutschen Behörden?

Die Fragen 7 bis 7e werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Auf die Antwort zu Frage 4 wird verwiesen.

8. Welche Abteilung bei Europol führt die angekündigte Untersuchung durch, und welche weiteren Partner, etwa private Firmen, sind daran beteiligt?

Bei Europol führt die Abteilung „Governance“ die Untersuchung durch. Daneben ist die niederländische Polizei und Justiz beteiligt

   a) Welche Parteien hatten nach Kenntnis der Bundesregierung nach jetzigem Stand der Erkenntnisse Einblick in die Daten?

Auf die Antwort zu Frage 4 wird verwiesen.

Vorabfassung - wird durch die lektorierte Version ersetzt.

b) Wann soll der Abschlussbericht der Untersuchung vorliegen?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

9. Welche weiteren Datenverluste von Agenturen der Europäischen Union (insbesondere Europol, Frontex, EASO und eu-LISA) sind der Bundesregierung aus den vergangenen fünf Jahren bekannt?

a) Welche Einstufungen trugen die Daten?

b) Wer war für die etwaigen Datenlecks verantwortlich, und auf welchem Weg bzw. über welche Datenträger gelangten die Daten nach außen?

c) Wie viele Personendatensätze enthielten die Daten?

d) Wie viele der abhandengekommenen Daten stammten von deutschen Behörden?

Die Fragen 9 bis 9d werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

10. Was ist der Bundesregierung darüber bekannt, auf welche Weise die Regierung Dänemarks sicherstellt, dass nach dem erfolgreichen Angriff auf dänische IT-Systeme, bei dem auch circa 1,2 Millionen Datensätze des Schengener Informationssystems (SIS) das Eindringen in die nationale SIS-Schnittstelle zumindest erschwert wird, indem, wie von der dänischen Polizei erklärt, die „ausgenutzte Sicherheitslücke“ geschlossen wurde (s. Plenarprotokoll 18/7)?

a) Welche Details über die Sicherheitslücke und die Art des Angriffs sind der Bundesregierung mittlerweile bekannt?

Die Fragen 10 und 10a werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Der Angriff auf das Schengener Informationssystem in Dänemark erfolgte unter Ausnutzung einer Sicherheitslücke in einem Webserver, mit deren Hilfe auf den Mainframe zugegriffen wurde. Nach Angaben der dänischen Polizei hat der IT-Dienstleister die entsprechende Sicherheitslücke nach Bekanntwerden geschlossen.

b) Was ist der Bundesregierung darüber bekannt, in welchen Ländern der externe IT-Dienstleister CSC, der zum Zeitpunkt des Angriffs neben anderen Anwendungen für die öffentliche Verwaltung Dänemarks auch das nationale Schengener Informationssystem Dänemarks betrieben hat, weitere EU-Datenbanken bzw. deren Schnittstellen betreibt?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

c) Was ist der Bundesregierung darüber bekannt, welche „Hintertür“ die Europäische Kommission der dänischen Regierung anbot, trotz des Referendums zum Ausstieg weiterhin bei der Polizeiagentur Europol mitarbeiten zu können („EU offers Denmark backdoor to Europol“, https://euobserver.com vom 8. Dezember 2016)?

Im Anschluss an die Erklärung des Präsidenten der Europäischen Kommission, Jean-Claude Juncker, des Präsidenten des Europäischen Rates, Donald Tusk, und des dänischen Ministerpräsidenten, Lars Løkke Rasmussen vom 15. Dezember

Vorabfassung - wird durch die lektorierte Version ersetzt.

2016 (IP-16-4398_DE) läuft derzeit das Verfahren zur Änderung des Beschlusses 2009/935/JI hinsichtlich der Liste der Drittstaaten und dritten Organisationen, mit denen Europol Abkommen schließen kann. Im Anschluss an die Ergänzung der Liste um Dänemark bestünde die Möglichkeit ein Abkommen zur Zusammenarbeit zwischen Europol und Dänemark zu schließen.

11. Welche Auswirkungen hat aus Sicht der Bundesregierung das Urteil des zweiten US-Berufungsgerichts vom 14. Juli 2016, das entschied, dass US-Cloud-Anbieter mit Sitz in Europa nicht aufgrund der bestehenden nationalen Gesetzgebung der USA gezwungen werden können, personenbezogene Daten ihrer Kunden herauszugeben, für die Strafverfolgungs- und Justizbehörden der EU, die ihrerseits Direktanfragen zur Herausgabe elektronischer Beweismittel bei Internetanbietern mit Sitz in den USA fordern?

Nach dem angesprochenen Urteil des betreffenden US Berufungsgerichtes (US Court of Appeals for the 2nd Circuit in New York) vom 14. Juli 2016 erstreckt sich die Verpflichtung von Microsoft als einem in den USA ansässigen Diensteanbieter zur Herausgabe von personenbezogenen Daten aufgrund einer Anordnung der US Strafverfolgungsbehörden nicht auf Daten, die in einem europäischen Rechenzentrum gespeichert sind. Auswirkungen auf Strafverfolgungsbehörden der EU Mitgliedstaaten ergeben sich daher für Konstellationen, in denen US Behörden im Wege der Rechtshilfe gebeten werden, entsprechende Daten bei in den USA ansässigen Diensteanbietern zu erheben. Erste Praxiserfahrungen dazu werden derzeit gesammelt.

a) Was ist der Bundesregierung über die Ergebnisse einer Prüfung dieser Auswirkungen durch die EU-Agenturen Eurojust oder Europol bekannt?

Der Bundesregierung liegen dazu keine Erkenntnisse vor.

b) Welche Verfahren und Strategien verfolgen der Rat und die Kommission derzeit für die Umsetzung der Möglichkeit von Direktanfragen bei Internetanbietern in den USA?

Auf die Beantwortung der Bundesregierung zur Schriftlichen Frage 31 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 18/8523 wird Bezug genommen. Die dort erwähnten Ratsschlussfolgerungen „Improving Criminal Justice in Cyberspace“ vom 9. Juni 2016 (Ratsdokument 10007/16) werden derzeit von der Europäischen Kommission umgesetzt. Dabei soll auch auf die direkte Kooperation zwischen Strafverfolgungsbehörden der EU-Mitgliedstaaten einerseits und in den USA ansässigen Diensteanbietern andererseits eingegangen werden. Konkrete Vorschläge der Kommission sind im Sommer 2017 zu erwarten.

12. Wie viele Datensätze enthalten die Europol-Arbeitsdateien „Hydra“ und „Travellers“ zum Stichtag 1. Dezember 2016, und wie viele Personen sind dort gespeichert?

Die Gesamtzahl der Datensätze im Auswerteschwerpunkt „Hydra“ beträgt 616 037 (Stand 1. Juni 2016) und im Auswerteschwerpunkt „Travellers“ 783 598 (Stand 31. Juni 2016.). Im Auswerteschwerpunkt „Hydra“ sind insgesamt 66 493 Personen, im Auswerteschwerpunkt „Travellers“ 33 076 Personen gespeichert (Stand 31. August 2016). Aktuellere Statistiken liegen der Bundesregierung nicht vor.

Vorabfassung - wird durch die lektorierte Version ersetzt.

13. Wie viele Datensätze enthält das Europol-Informationssystem zu „ausländischen terroristischen Kämpfern“, und wie viele Personen sind dort gespeichert?

Das Europol-Informationssystem enthält 13 645 terrorismusbezogene Objekte, 6 506 „ausländische Kämpfer“ oder Unterstützer sind gekennzeichnet (Stand 4. Oktober 2016). Insgesamt enthält das Europol-Informationssystem 106 493 Personen (Stand 4. Oktober 2016).

14. Was ist der Bundesregierung darüber bekannt, inwiefern die „Meldestelle für Internetinhalte“ („EU Internet Referral Unit“) bei Europol die Möglichkeit umsetzen wird, gemäß der neuen Europol-Verordnung (ABl. L 153 vom 24. Mai 2016, S. 35) ab dem 1. Mai 2017 auch mit privaten Firmen Personendaten auszutauschen?

Die Bundesregierung hat keine Kenntnis, zu welchem Zeitpunkt nach dem 1. Mai 2017 die „Meldestelle für Internetinhalte“ bei Europol mit privaten Stellen personenbezogene Daten gemäß der neuen Europol-Verordnung (EU) 2016/794 austauschen wird. Sie geht jedoch davon aus, dass Europol von ihr durch die Europol-Verordnung eingeräumten Befugnissen Gebrauch machen wird.

a) Wie viele der gefundenen Internetinhalte zu „Extremismus/Terrorismus“ und „illegale Migration“ fand die Meldestelle durch eigene Recherchen, und wie viele stammten von Behörden der Mitgliedstaaten?

Auf die Antwort der Bundesregierung zu den Fragen 19, 19a und 20 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/10591 wird verwiesen. Weitere Erkenntnisse liegen der Bundesregierung nicht vor.

b) Inwiefern wird auf EU-Ebene darüber diskutiert, die Zuständigkeit der Meldestelle auf andere Kriminalitätsphänomene bzw. Erscheinungsformen von „Hate Speech“ auszuweiten, und welche Haltung vertritt die Bundesregierung hierzu?

Auf die Antwort der Bundesregierung zur Schriftlichen Frage 13 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 18/10773 wird verwiesen.

15. Was ist nach Kenntnis der Bundesregierung damit gemeint, wenn ein Sprecher von Europol gegenüber dem Sender ZEMBLA davon spricht, Europol verfüge über ein „sehr robustes System“, um die gespeicherten Informationen zu schützen?

Auf die Antwort zu Frage 1 wird verwiesen.

16. Was ist der Bundesregierung über die Beschaffenheit eines neuen Geheimschutzraums bei Europol bekannt, und aus welchem Grund wurde dieser eingerichtet?

Die Bundesregierung hat hierzu keine Erkenntnisse.

Vorabfassung - wird durch die lektorierte Version ersetzt.

17. Was ist der Bundesregierung darüber bekannt, aus welchem Grund der noch amtierende Europol-Direktor Rob Wainwright wie von BBC berichtet an einem Seminar zu Onlinesicherheit und Datenschutz teilnimmt?

Die Webseite des Veranstalters führt den Europol-Direktor als Vortragenden. Darüber hinaus hat die Bundesregierung zu den Gründen für die Teilnahme keine Erkenntnisse.

Vorabfassung - wird durch die lektorierte Version ersetzt.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333